New Cyber Law, Pending Details: Critical Infrastructure Must Report Cyber Breaches, Ransom Payments

CISA to develop specific cyber incident reporting requirements by March 2024

By Susan Lindberg, Trent Shores, and Tom Vincent
March 21, 2022

President Biden's recent signature of a new cyber incident reporting law made headlines. The Cyber Incident Reporting for Critical Infrastructure Act of 2022, which was attached to a $1.5 trillion government funding bill, requires critical infrastructure owners to file a report with the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security if they have been hacked or made a ransom payment in response to a ransomware attack. Reports must be made within 72 hours of a breach, and within 24 hours of a ransom payment.

The statute, signed March 15, 2022, requires CISA to issue rules implementing the new law. CISA has two years to publish its proposed rules in the Federal Register. The law does not provide specific guidance on whether, how, or in what circumstances to report cyber incidents in the interim. The U.S. government has consistently urged, but not required, critical infrastructure owners to report significant incidents. For example, the Cybersecurity Information Sharing Act of 2015.

Who will be affected? The law applies to "covered entities" within the 16 critical infrastructure sectors identified in Presidential Policy Directive 21, which was issued in 2013. These sectors are: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems. The new law requires CISA's rule to include a clear description of the types of entities that constitute "covered entities."

What types of incidents must be reported? Covered entities must report "covered cyber incidents." At a minimum, these are:

i. a cyber incident that leads to substantial loss of confidentiality, integrity or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;
ii. a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack or exploitation of a zero day vulnerability; or
iii. unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise.

The new statute directs CISA to clearly describe the types of incidents that are "covered cyber incidents."

Ransom payments in connection with a covered cyber incident must also be reported.

How will reported information be used? Information will be anonymized, aggregated, and shared among various government agencies in order to improve cybersecurity, identify and track attackers, and assist companies in addressing ongoing threats and vulnerabilities.

Will companies be penalized if they do not report? The new law does not give CISA the authority to issue fines or other penalties. It specifically grants CISA the power to issue subpoenas to allow it to obtain information to companies that do not submit a required report.

Does information provided to the government remain private? Companies reporting cyber incidents or ransom payments to CISA will receive protections similar to those contained in the Cybersecurity Information Sharing Act of 2015: companies receive liability protections, privileges are maintained, proprietary information is protected, information is not released under the Freedom of Information Act, and certain liability protections.

How to plan ahead for required reporting? Although the details of CISA's reporting requirements are not yet known, because other laws and regulations in effect (as well as client or vendor contracts) may require an organization to report a significant cyber incident within a short period of time to the government or to others, organizations should (if they haven't already) have both a reporting plan in place and a structure to appropriately collect information for such reporting.

Sources of these reporting requirements may include:

- Securities and Exchange Commission reporting requirements -- in addition to its 2018 guidance on reporting of cyber incidents, the SEC has proposed a new regulation on cybersecurity requirements and disclosure
- State data privacy laws
- Industry-specific regulations, such as the TSA Security Directives for critical pipeline infrastructure
- Insurance policies

An organization will have many decisions to make within a short time frame if it experiences a significant cybersecurity breach. It is important to know and consider ahead of time what circumstances would require reporting, and include those requirements and outline a decision process in an incident response plan. Seek advice of counsel for guidance on the specific requirements applicable to your organization.

Regardless of whether a disclosure is required by law, an organization may wish to make voluntary disclosures, either to government agencies or to an information sharing and analysis center specific to the industry, or to law enforcement or the organization's insurance carrier. Legal counsel can provide guidance on ensuring that the organization is protected when providing such information.

Susan Lindberg
Former General Counsel and candidate for Master of Science — Cybersecurity
918-595-4826
slindberg@gablelaw.com

Trent Shores
Former United States Attorney and National Security Cyber Specialist
918-595-4805
tshores@gablelaw.com

Tom Vincent
Certified Regulatory Compliance Manager and Certified Information Privacy Professional
918-595-4857
tvincent@gablelaw.com